UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/966,777	09/28/2001	David A. Lee	42390P11152	5083

7590 02/14/2006

BLAKELY, SOKOLOFF,
TAYLOR & ZAFMAN LLP
Seventh Floor
12400 Wilshire Boulevard
Los Angeles, CA 90025-1026

EXAMINER	
SCHUBERT, KEVIN R	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 02/14/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/966,777	LEE ET AL.	
	Examiner	Art Unit	
	Kevin Schubert	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 January 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,5-9,19,20,23,25,26,28,29,32,33,35 and 36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,5-9,19,20,23,25,26,28,29,32,33,35 and 36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-2,5-9,19-20,23,25-26,28-29,32-33, and 35-36 have been considered. Examiner has fully considered applicant's remarks, presented 1/27/06, but respectfully disagrees and maintains the rejections of the previous action.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 1-2,5-9,19-20,23,25-26,28-29,32-33, and 35-36 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The examiner finds no support for the newly amended limitation "encrypting each of the update keys using the corresponding secret key assigned to each of the valid receivers".

Having fully considered the specification, the examiner finds support for "update keys encrypted *using secret keys assigned to each receiver*" (specification: [0026]). The examiner also finds support that "update keys are encrypted with a key that is a combination of the previous update key, the device secret key associated with this row or column, and table location" (specification: [0036]). However, the examiner finds no support for the limitation "encrypting each of the update keys using the corresponding secret key assigned to each of the valid receivers" as claimed. Appropriate correction or a specific reference pointing out specifically where this limitation is disclosed in the specification is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-2,5-9,19-20,23,25-26,28-29,32-33, and 35-36 are rejected under 35 U.S.C. 102(b) as being anticipated by Lotspiech, U.S. Patent No. 6,118,873.

As per claims 1-2,5-9,19-20,23,25-26,28-29,32-33, and 35-36, the applicant discloses a method comprising the following limitations which are met by Lotspiech:

a) generating a list of update keys on a key distribution center system based on a table of secret keys identifying the valid and invalid receivers of a plurality of receivers, the list of update keys allowing valid receivers to decrypt a valid content key using update keys obtained from the list of update keys (Col 5, lines 9-19);

b) generating a multiple nested list of decryption patterns based on the list of update keys (Col 2, lines 7-41);

c) encrypting each of the update keys using the corresponding secret key assigned to each of the valid receivers (Col 2, lines 7-41);

d) broadcasting the multiple nested list of decryption patterns to the plurality of receivers (Col 2, lines 7-41);

e) recovering a content key from the list of update keys by recovering a set of update keys for each receiver from the multiple nested list of decryption patterns and using the set of update keys to decrypt the content key, wherein the valid receivers receive the recovered content key to facilitate decryption of content, and each of the invalid receivers to receive an intermediate key indicating to the key distribution center that an invalid receiver is to have the content blocked to facilitate blocking of the content (Col 2, lines 7-41; Col 6, line 58 to Col 7, line 45);

Lotspiech discloses a method of broadcasting a content key to a valid receiver in which each receiver maintains a plurality of device keys and a licensing agency keeps a list which identifies the secret keys of all receivers. To broadcast a content key, a licensing agency generates a list of session numbers (update keys) which are encrypted with respective secret keys of receivers. The encrypted list of session numbers is combined into a session key block which is broadcast to a plurality of receivers. Valid receivers use their respective keys to decrypt the session numbers (update keys) which are then used to decrypt the content key. However, if an invalid receiver is identified, a compromised key of the compromised device is identified from the table of secret keys and used to encrypt a dummy number which prevents the invalid receiver from arriving at the content key and instead makes him arrive at a distinct second key.

Claims 1-2,7-9,19-20,23,25-26,28-29,32-33, and 35-36 are rejected under 35 U.S.C. 102(b) as being anticipated by Richards, U.S. Patent No. 6,069,957.

As per claims 1,19, and 28, the applicant describes a method comprising the following limitations which are met by Richards:

a) generating a list of update keys on a key distribution center system based on a table of secret keys identifying valid and invalid receivers of a plurality of receivers, the list of update keys allowing valid receivers to decrypt a valid content key using update keys obtained from the list of update keys (Col 4, lines 52-67; Col 9, lines 12-31);

b) generating a multiple nested list of decryption patterns based on the list of update keys (Col 9, lines 12-31);

c) encrypting each of the update keys using the corresponding secret key assigned to each of the valid receivers (Col 9, lines 12-31);

d) broadcasting the multiple nested list of decryption patterns to the plurality of receivers (Col 1, lines 25-31);

e) recovering a content key from the list of update keys by recovering a set of update keys for each receiver from the multiple nested list of decryption patterns and using the set of update keys to decrypt the content key, wherein the valid receivers receive the recovered content key to facilitate decryption of content, and each of the invalid receivers to receive an intermediate key indicating to the key distribution center that an invalid receiver is to have the content blocked to facilitate blocking of the content (Col 9, lines 12-31; Col 10, lines 33-48).

As per claims 2,20, and 29, the applicant describes the method of claims 1,19, and 28, which are met by Richards (see above), with the following limitation which is also met by Richards:

Wherein the generating of the list of update keys comprises generating one or more distinct intermediate keys and the content key (Col 9, lines 12-31);

As per claims 7 and 25, the applicant describes the method of claims 1 and 19, which are met by Richards (see above), with the following limitation which is also met by Richards:

Wherein the recovering a set of update keys for each receiver from the multiple nested list of decryption patterns comprises parsing the multiple nested list of decryption patterns to locate an entry intended for a particular receiver based on detection of a predetermined test pattern included in an entry in the multiple nested list of decryption patterns (Col 9, lines 63-67);

As per claims 8,26, and 35, the applicant describes the method of claims 1,19, and 28, which are met by Richards (see above), with the following limitation which is also met by Richards:

Further comprising broadcasting the content encrypted with the content key (Col 9, lines 26-31).

As per claims 9 and 36, the applicant describes the method of claims 8 and 35, which are met by Richards (see above), with the following additional limitation which is also met by Richards:

Further comprising decrypting said content encrypted with said content key using a content key recovered from the multiple nested list of decryption patterns (Col 9, lines 26-31).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 5-6,23, and 32-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Richards in view of Uz, U.S. Patent No. 6,351,538.

As per claims 5,23, and 32, the applicant describes the method of claims 1,19, and 28, which are met by Richards (see above), with the following limitation which is met by Uz:

Wherein the generating a multiple nested list of decryption patterns comprises encrypting an entry of the list of update keys using a key that comprises a combination of a previous update key, a secret key for a receiver associated with the entry of the list of update keys, and an index indicating a location in the table of secret keys associated with each entry (Uz: Col 8, lines 25-31; Richards: Col 9, lines 12-31);

Richards discloses all the limitations of claims 1,10,19,28,37, and 42. Richards fails to disclose an "index indicating a location in said table of secret keys associated with each entry". Uz discloses a one way broadcasting system which broadcasts key and content information for conditional access systems, such as a pay-per-view system. Uz system also discloses the use of maintaining key tables. Furthermore, Uz discloses the idea of transmitting an index indicating a location in the table of secret keys which can be used to locate keys for decryption.

It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Uz with those of Richards and incorporate the use of an index indicating a location in a table of secret keys so that the receiver can use the index to locate secret keys for decryption.

As per claims 6 and 33, the applicant describes the method of claims 5 and 32, which are met by Richards (see above), with the following additional limitation which is met by Uz:

Wherein an entry in the multiple nested list of decryption patterns includes a predetermined test pattern encrypted with the secret keys for a receiver associated with the entry of the list of update keys (Col 9, lines 63-67);

Richards discloses all the limitations of claims 5 and 32. However Richards fails to disclose the use of encrypting the predetermined test pattern with the secret keys for a receiver. Uz discloses a one way broadcasting system which broadcasts key and content information for conditional access systems, such as a pay-per-view system. Furthermore, Uz discloses the idea of encrypting header information (Col 6, lines 13-14).

It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Uz and Richards and encrypt the header of information of Richards' system because doing so would make the system more secure and less vulnerable to hackers being able to intercept the broadcast and know information about the data.

Response to Arguments

Applicant's arguments, see Remarks filed 1/27/06, with respect to the 112, first paragraph, rejection of all pending claims have been fully considered but they are not persuasive. Applicant argues that the amendments overcome the rejection. Examiner respectfully disagrees.

The issue in the previous action was whether Applicant had disclosed the limitation "encrypting each of the update keys using the corresponding secret key assigned to each of the valid receivers". Examiner stated that, after careful consideration of the Specification, Examiner was able to find support for "update keys encrypted *using secret keys assigned to each receiver*" ([0026]). Examiner also found

that "update keys are encrypted with a key that is a combination of the previous update key, the *device secret key associated with this row or column*, and table location" ([0036]). Thus, it is clear that Applicant has disclosed that update keys are encrypted using secret keys of each receiver, and that an update key is encrypted using a secret key associated with the particular row or column.

In contrast, Examiner does not find support for "encrypting each of the update keys *using the corresponding secret key assigned to each of the valid receiver*". Applicant's addition of the new limitation an intermediate key "indicating to the key distribution center that an invalid receiver is to have the content blocked" does not rectify the situation. Accordingly, the 112, first paragraph, rejection of all claims is maintained.

Applicant's arguments with respect to the 102(b) rejection of all pending claims under Lotspiech have been fully considered but they are not persuasive. Applicant appears to be arguing that the newly added limitation, "each of the invalid receivers to receive an intermediate key indicating to the key distribution center that an invalid receiver is to have the content blocked to facilitate blocking of the content", is not disclosed by Lotspiech because Lotspiech discloses that device keys are used in an encryption module.

Examiner respectfully disagrees with this argument. Lotspiech's disclosure of using device keys in an encryption module does not appear to have bearing on an invalid receiver receiving an intermediate key. In fact, Lotspiech discloses that when a key distribution center determines that an invalid receiver is compromised, the key distribution center may configure a session key block such that an invalid receiver is to receive an intermediate key to facilitate blocking of content. For example, Lotspiech teaches the following:

"On the other hand, when the licensing agency has determined that at least one device 18 has been compromised, the agency accesses the subset of device keys that had been assigned to the compromised device, and then proceeds from decision diamond 60 to block 64 to identify at least one key position, e.g., the ith key position, of the compromised device in which the particular device key S_{ji} that has been assigned to the compromised device resides. It is to be understood that for clarity of disclosure, it is assumed that only a single device key position of the compromised device is selected as described below. The principles below, however, can be applied to select two or more device key positions and process them simultaneously.

Moving to block 66, the logic envisions encrypting all non-I session numbers x_{non-I} with all non-j (relative to the device key S_{ji} of the compromised device 18) corresponding device keys $S_{non-j, non-I}$ in accordance with principles discussed above. Also, at block 68 the ith session number x_i is encrypted with all non-j device keys $S_{non-j,i}$. This leaves, as the only session block matrix element left for encryption, the session number at the location at which the selected comprised device key $S_{j,I}$ happens to be.

Accordingly, at block 70 a number is encrypted using the selected compromised $S_{j,I}$, but the number is not the ith session number x_i. Rather, it is a dummy number 'y'. A session key block 72 in Fig. 8 is substantially identical to the session key block 42 shown in Fig. 5 and generated by the logic of Fig. 4, except that the session key block 72 in Fig. 8 includes a dummy position 76, representing an encrypted version of the dummy number 'y'" (Col 6, line 58 to Col 7, line 23).

Accordingly, the rejection is maintained.

Applicant's arguments with respect to the 102(b) rejection of all pending claims under Richards have been fully considered but they are not persuasive. Applicant appears to be arguing that Richards teaches distributing encrypted decryption keys, and, in contrast, does not teach applicant's newly added claimed limitation "each of the invalid receivers to receive an intermediate key indicating to the key distribution center that the invalid receiver is to have the content blocked to facilitate blocking of the content". Such an argument is not persuasive on any level.

It is respectfully submitted that claim 1, itself, calls for distributing encrypted decryption keys. As such, Examiner is somewhat bewildered as to Applicant's argument that Richards teaching of distributing encrypted decryption keys is in contrast to Applicant's newly added claim limitation. In any event, Examiner respectfully notes that Richards discloses generating a list of update keys on a key distribution center system based on a table of secret keys identifying the valid and invalid receivers of a plurality of receivers. Further, Richards discloses generating and broadcasting a multiple list of decryption patterns based on the list of update keys. Furthermore, the key distribution center generates and broadcasts the multiple list of decryption patterns such that a valid receiver is to receive a content key to facilitate decryption and an invalid receiver is to receive an intermediate key to facilitate blocking of the content. Thus, the rejection is maintained.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kevin Schubert whose telephone number is (571) 272-4239. The examiner can normally be reached on M-F 7:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KS

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER